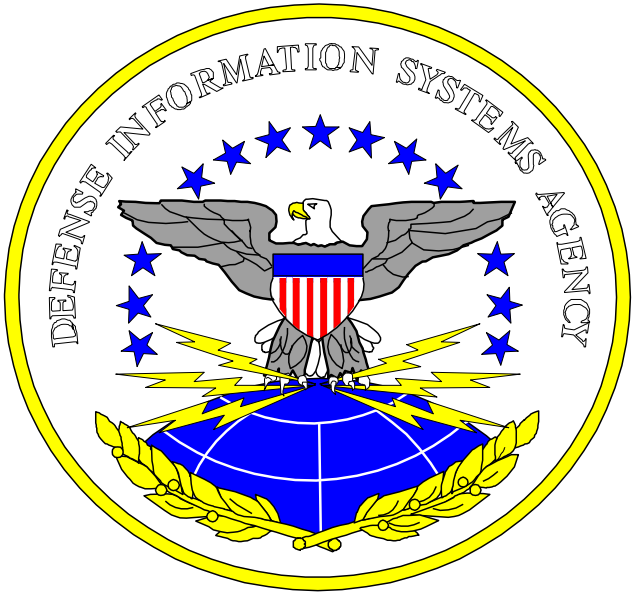
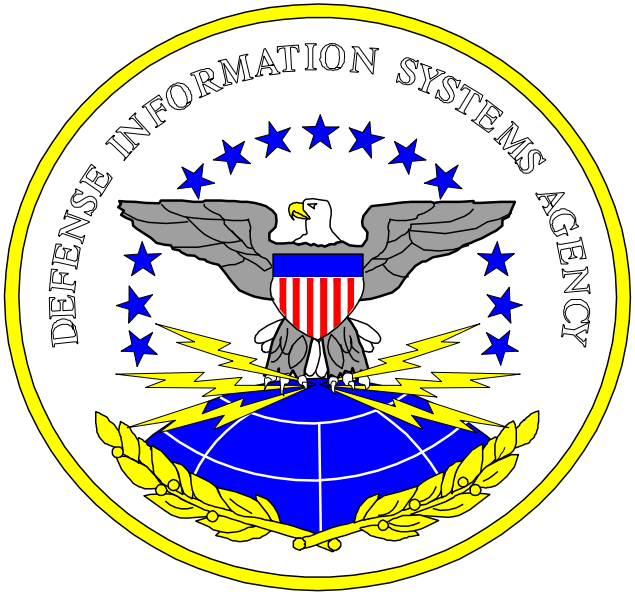


DII COE 4.x Security

LTC Alex Froede
Defense Information Systems Agency
DII COE Engineering Office
(703) 735-8509 froedea@ncr.disa.mil

Agenda

- **Overview** — **LTC Alex Froede**
- **COE 4.x Security Baseline** — **LTC Alex Froede**
- **Security Requirements in the New COE 4.0 I&RTS** — **Matt O'Brien**
- **Security Banner** — **Erik King**
- **COE 4.x Security Services Architecture** — **Erik King**
- **Demo of Security Prototype Tool: Security Module for VerifySeg** — **Jack Lawrence**



OVERVIEW

LTC Alex Froede
Defense Information Systems Agency
DII COE Engineering Office
(703) 735-8509 froedea@ncr.disa.mil

COE 4.X Out-Of-The-Box Security

- **COE 4.X will install in a default “lock-down” security configuration (COE 4.x Security Baseline). Details in next briefing.**
- **Default based on requirements in Security Services SRS and results of security evaluations of the COE kernel.**
- **Some COE 3.x applications may not operate in the new COE 4.x Security Baseline environment.**
- **Intent is to force System Integrators and Program Managers to make a conscience decision to relax the security baseline of the COE and/or to use applications that cannot operate in this new security environment.**

COE 4.x Security Documentation for Developers

- **DII COE Kernel Developers Security Guide, Unix version**
  - **Now available from COE Security web page**
- **DII COE Kernel Developers Security Guide, Window NT version**
  - **Available in May 99**
- **DII COE Security Features Developer's Guides**
  - **Unix and Windows NT version available in early July 99**
- **DII COE 4.0 I&RTS. Significant Security updates made over previous version**
  - **Draft available now**

COE 4.x Security Documentation for Developers (Continued)

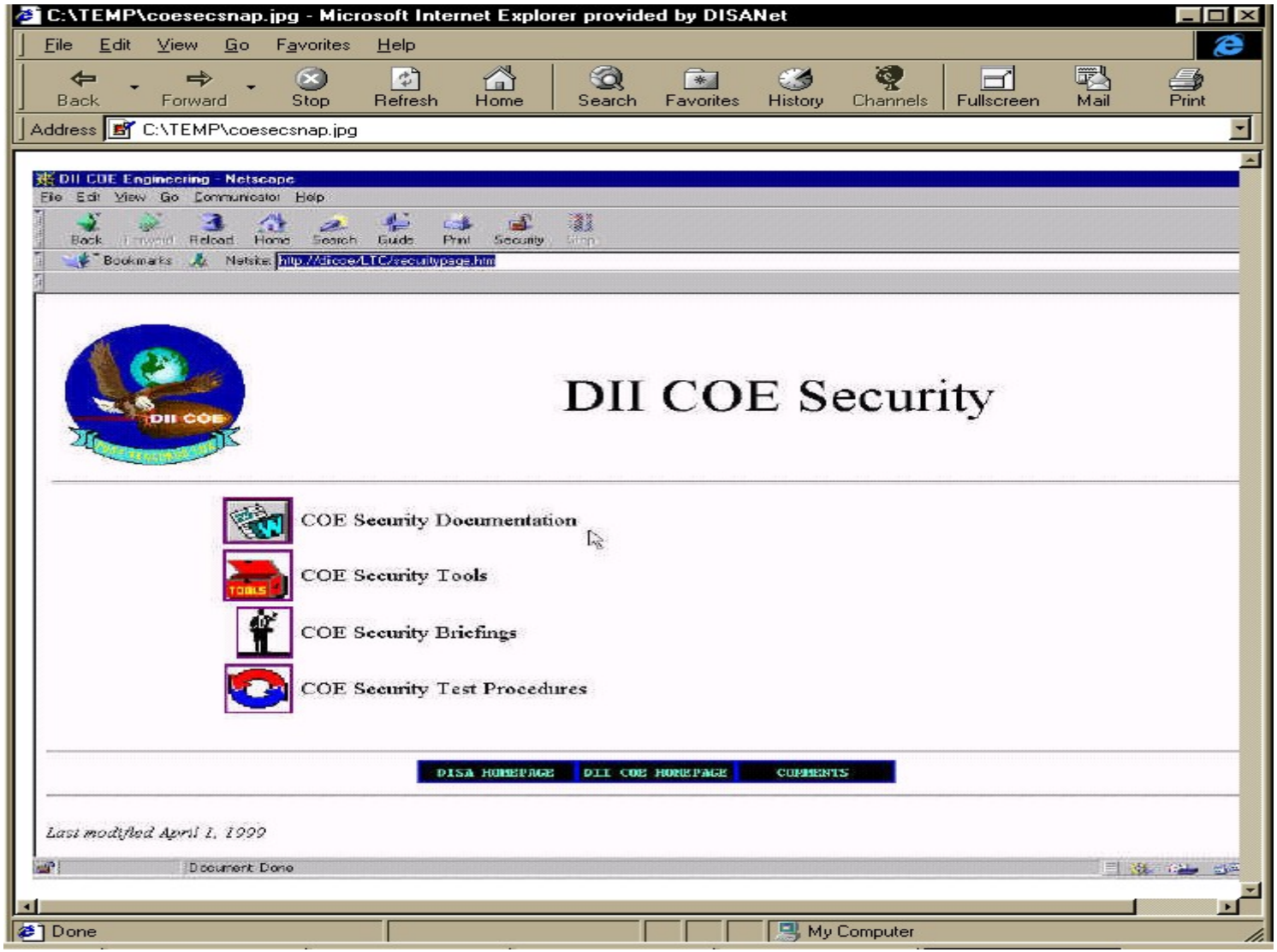
- **DII COE Security Configuration and Installation Guide, Windows NT for COE 4.x. Update of previous guide to add considerations for new COE security baseline and the inclusion of Windows SP4 in COE 4.x.**
  - **Available in June 99**
- **DII COE Security Configuration and Installation Guide, Unix for COE 4.x. Update of previous guide to add considerations for new COE security baseline.**
  - **Available in June 99**
- **DII COE 4.x Security Test Procedures**
  - **Available May 99**

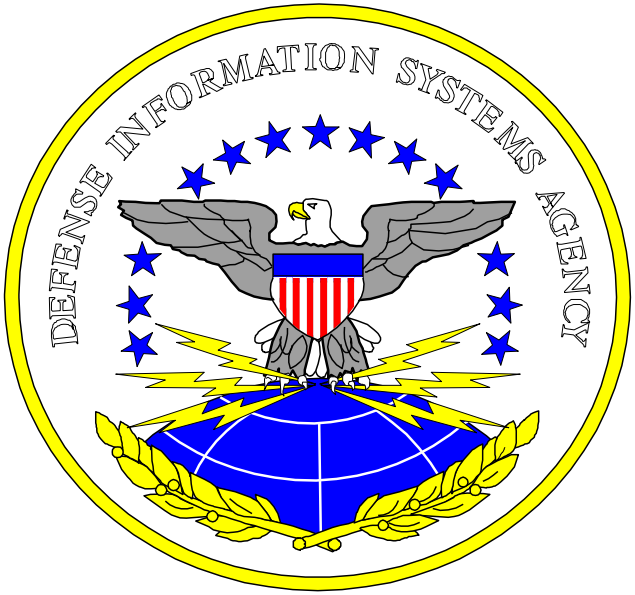
COE 4.x Security Tools

- **Update versions of the automated DII COE security configuration tools will be released by Oct 99**
- **A security module will be added to the VerifySeg tool**
  - **Purpose is to provide an automated capability to check compliance with the security requirements of the new COE 4.0 I&RTS.**
  - **Module designed to be run before and after segment installation.**
  - **The tool will check security compliance in two passes IAW two separate compliance requirements tables**
  - **The first table will include the DII COE Chief Engineer minimal security compliance requirements (I&RTS App B)**
    - **Compliance violations can be set to a strict pass/fail criteria or to produce warnings**
  - **The second table is optional and is configured by the system Chief Engineer or integrator**
    - **Only warnings are issued for violations**
  - **Results of the security compliance check will be provided at all segment deliveries.**

"New" & "Improved" COE Security Web Site

- **The majority of all DII COE Security documents and tools will be available through the recently updated COE security web page found by selecting the Security link from the DII COE Engineering home page**


C:\TEMP\coesecsnap.jpg - Microsoft Internet Explorer provided by DISANet
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address C:\TEMP\coesecsnap.jpg
DII COE Engineering - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Netsite: http://jfcoe/LTC/securitypage.htm
DII COE Security
COE Security Documentation
COE Security Tools
COE Security Briefings
COE Security Test Procedures
DISA HOMEPAGE
DII COE HOMEPAGE
COMMENTS
Last modified April 1, 1999
Document Done
Done
My Computer



Security Baseline for COE 4.x

LTC Alex Froede
Defense Information Systems Agency
DII COE Engineering Office
(703) 735-8509 froedea@ncr.disa.mil

UNIX Kernel Changes (Samples)

COE 3.x

- **User's search path includes current directory and user's home directory**
- **Audit log security**
  - **config. files world-readable**
  - **events logged**
  - **minfree set to 20**
- **Network services set to vendor defaults**

COE 4.x

- **Removes "." and "$HOME" from /h/COE/Scripts/.cshrc.COE**
- **Audit log security**
  - **No world access**
  - **Improved event collection**
  - **minfree set to 15**
- **Network services limited**
  - **empty /.rhosts file with a permission of 600**

UNIX Kernel Changes (Samples)

COE 3.x

- **UMASK 002**
- **SUID/SGID shell scripts**
- **All segments in account-group have same access control policy**

COE 4.x

- **umask for root and all new users is now 022, 027 being considered**
- **Many SUID/SGID scripts rewritten as binaries**
- **No account-groups therefore developer and site administrator set access control policy for each segment**

UNIX Kernel Changes (Samples)

COE 3.x

- **World-writeable files and directories**

COE 4.x

- **Kernel will ship with permissions locked down**
  - **/etc/vfstab is not world writable**
  - **verifySeg will flag world writable files**
  - **/tmp has sticky bit set**
  - **Tighter permissions for secman and sysadm**

NT Kernel Security (Samples)

COE 3.x

- NT 4.0 OS (no SP or hotfixes)
  - Sites responsible for obtaining and installing SP3 and post-SP3 hotfixes
- Securing systems was time-intensive manual process
  - Secure NT I&C Guide

COE 4.x

- NT 4.0 OS with SP4 OS patch
  - Coordinating with JPL to include post-SP4 hotfixes in OS patch
- Goal is to deliver secure system (schedule impact)
  - JPL reviewing Secure I&C Guide and evaluating best method to secure systems
  - Security Configuration Manager templates can be used to secure system and/or applications

NT Kernel Security (Samples)

COE 3.x

- I&RTS did not address NT-specific application security issues

COE 4.x

- I&RTS updated to include
  - NT apps must be Microsoft logo-compliant
  - VeriTest Analyzer results must be submitted as part of the segmentation process
  - NT apps must execute on a securely configured OS

Other Security Changes

- **Kernel**
  - **edit local hosts now uses IP rather than hostname**
- **Security Programming Guidance**
  - **Guides for Unix and NT (MITRE)**
- **5.0 installer will enforce Chief Engineer Approval required to use some descriptors. (e.g., run post-install as a trusted user, chown in post-install.)**
  - **design your segments with this in mind NOW**

Security in the DII COE 4.0 I&RTS

Matt O'Brien
obrienma@saic.com

31 March 1999

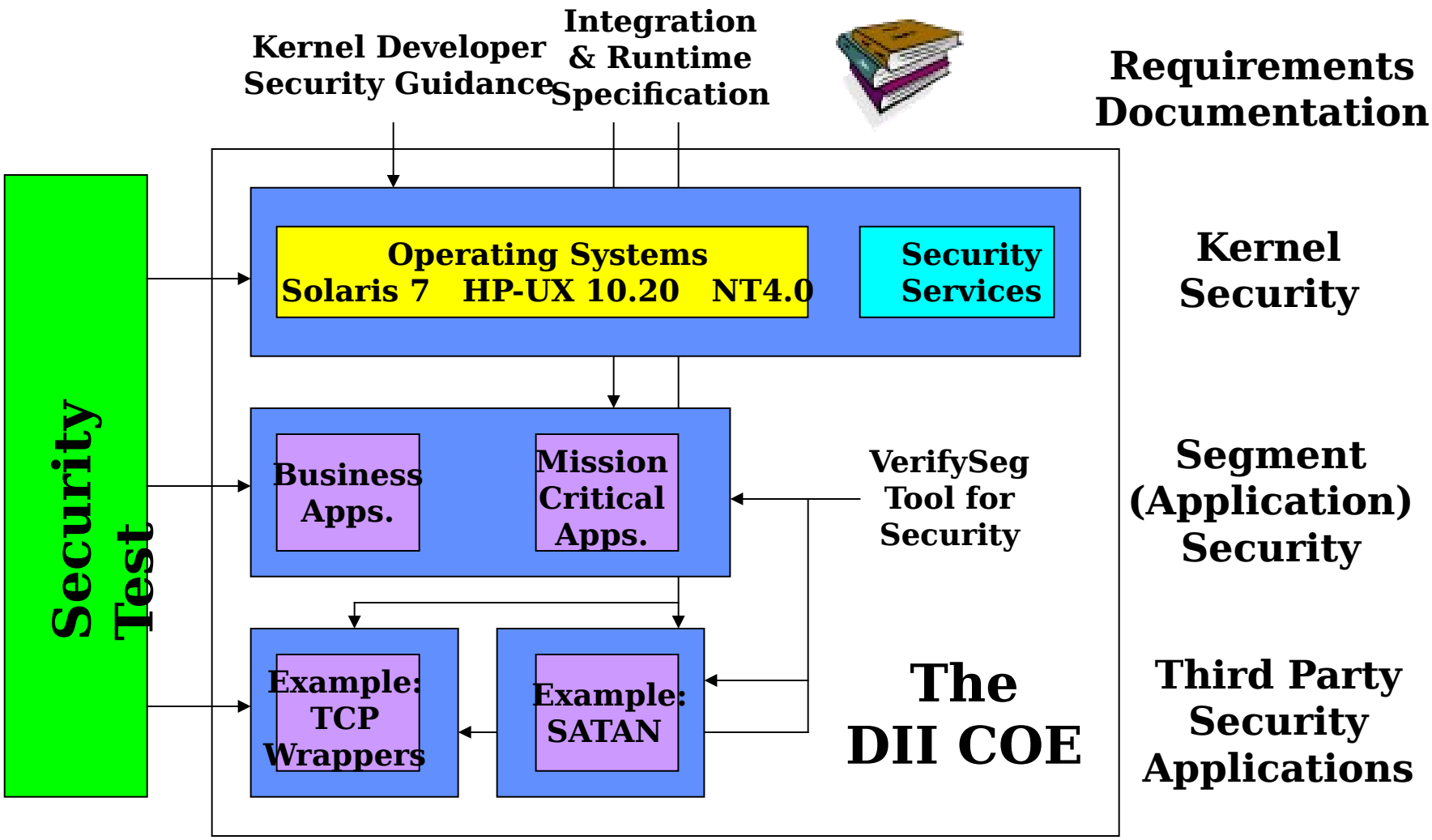
Overview

Many shall be restored that now are fallen
and many shall fall that now are in honor.

Horace, *Ars Poetica*

- Systems security engineering approach
- Separate chapter for security
- Significant security requirements for Level 5 compliance (and above)

Security in DII COE 4.x



Chapter 4: DII COE Security

- Integration and Runtime perspective

- Discussion of Certification and Accreditation
  - Relation to compliance requirements
  - VerifySeg tool to assist developers

- COE Security Services
  - /h directory structure
  - umask restriction
  - PATH statement restriction
  - Restricted user environment (UNIX)
  - Network services restrictions (UNIX)

Chapter 4: DII COE Security (cont.)

- COE Security Services (cont.)
  - Security Services APIs
  - Command-line Access restriction
- File and Directory permissions
- Shell script restrictions (UNIX)

Appendix B Compliance Requirements

Level 5

T	F	N/A	5-1	If an aggregate segment, the security level of the parent segment dominates the security level of the child segments.
T	F	N/A	5-2	For COE-component segments, if the segment provides a command-line mode or feature, the DII COE Chief Engineer has granted prior approval. The `$CMDLINE` keyword is used in the `Direct` segment descriptor to indicate command-line access is provided.
T	F	N/A	5-3	For mission-application segments, if the segment provides a command-line mode or feature, the Chief Engineer has granted prior approval. The `$CMDLINE` keyword is used in the `Direct` segment descriptor to indicate command-line access is provided.
T	F	N/A	5-4	The segment does not provide a "back door" access to a command-line prompt. If a command-line mode is available, it is through a known, documented approach for all authorized users and not through some hidden, undocumented approach.
T	F	N/A	5-5	For all segments, whether COE-component segments or mission-application segments, prior approval has been granted by the Chief Engineer to provide a command-line mode or feature that allows "superuser" access. The `$CMDLINE` and `$SUPERUSER` keywords are used in the `Direct` segment descriptor to indicate superuser access.
T	F	N/A	5-6	Entering a command-line mode requires the operator to enter a password and forces execution of the system login process.
T	F	N/A	5-7	If privileged user permissions are required during segment installation or removal, the Chief Engineer has granted prior approval.
T	F	N/A	5-8	The segment contains no directories or files, nor does it create directories or files, at install time or runtime that grant world write permissions. `VerfiySeg` will strictly fail any segment that violates this requirement.
T	F	N/A	5-9	The segment does not insert the current working directory (e.g., ".") nor "~" into the runtime search path for executables. `VerifySeg` will strictly fail any segment that violates this requirement. This rule does not apply to `PostInstall`, `PreInstall`, or `DEINSTALL` descriptors or other scripts that are used only during the installation/deinstallation process, nor to scripts used only in a software development environment.
T	F	N/A	5-10	The segment contains only subdirectories directly underneath the segment's home directory. No files are contained in the segment's home directory.
T	F	N/A	5-11	(UNIX) The segment uses GIDs that were assigned at segment registration time. The GID is segment specific, based on the segment prefix, and is used by the segment to restrict unauthorized access to the segment or its data.
T	F	N/A	5-12	(UNIX) If the segment uses the COE GID, the DII COE Chief Engineer has authorized such usage.
T	F	N/A	5-13	(UNIX) The segment does not alter the `umask` setting[1] established by the COE for the runtime environment.
T	F	N/A	5-14	(UNIX) The segment does not contain or create any shell scripts that `SUID` or `SGID` to root. `VerifySeg` will strictly fail any segment that violates this requirement.
T	F	N/A	5-15	(UNIX) The segment does not contain or create C shell scripts. The Bourne or Korn shell is used for shell scripts. `VerifySeg` will strictly fail any segment that uses C shell scripts.
T	F	N/A	5-16	(NT) The segment has no directories or files that grant `ALL` permissions to the "Everyone" or "Domain Guests" groups.

Appendix B
Compliance Requirements

Level 6

T	**F**	**N/A**	**6-1**	If the data for a particular segment contains any classified entries, then all of its data is packaged in a separate data segment and classified accordingly.
T	**F**	**N/A**	**6-2**	Classified segments are packaged separately from unclassified segments, or from segments which are classified at a lower level. (It is permissible to create aggregate segments, or segment suites, that contain segments at different classification levels, but the aggregate/suite must be labeled with the highest classification level of any segment within the aggregate/suite.)
T	**F**	**N/A**	**6-3**	Termination of segment execution, whether premature, inadvertent, or intentional does not place the operator at a command-line prompt.
T	**F**	**N/A**	**6-4**	Privileged processes, if required, have been authorized by the Chief Engineer and are listed in the `Processes` segment descriptor. (If the product is a COTS product that starts its own background processes instead of using the `Processes` descriptor, the processes started must be documented in the *SVD* document or its equivalent, and a waiver granted by the Chief Engineer.)
T	**F**	**N/A**	**6-5**	(UNIX) No directory or file permission, whether created at install time or runtime, is less restrictive than identified in the Security chapter's directory/file permissions table, unless authorized by the Chief Engineer. Any such directories or files that do not meet the permissions identified in the table are documented in the *SVD* document or its equivalent. `VerifySeg` uses this table to check permissions and all warnings from the check are explained in the `VSOutput` file.
T	**F**	**N/A**	**6-6**	(NT) If the segment creates groups, the groups follow the naming conventions in the Windows New Technology (NT)-Based Segments chapter.